9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2023-0019]

Agency Information Collection Activities: CISACare Questionnaire, Provided via CISACare.gov

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS).

ACTION: 60-day notice and request for comments on a new collection.

SUMMARY: The Cyber Security Division's Vulnerability Management Sub-Division (CSD VM) within Cybersecurity and Infrastructure Security Agency (CISA) will submit the following Information Collection Request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

DATES: Comments are encouraged and will be accepted until ***[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].***

ADDRESSES: You may submit comments, identified by docket number Docket # CISA-2023-0019, at:

- Federal eRulemaking Portal: http://www.regulations.gov. Please follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name and docket number Docket # CISA- 2023-0019. All comments received will be posted without change to http://www.regulations.gov, including any personal information provided.

Docket: For access to the docket to read background documents or comments received, go to http://www.regulations.gov.

SUPPLEMENTARY INFORMATION: Consistent with CISA's authorities to "carry out comprehensive assessments of the vulnerabilities of the key resources and critical

infrastructure of the United States" at 6 U.S.C. 652(e)(1)(B) and provide Federal and non-Federal entities with "operational and timely technical assistance" at 6 U.S.C. 659(c)(6) and "recommendation on security and resilience measures" at 6 U.S.C. 659(c)(7), CSD VM's CyberCare initiative will collect information in order to provide tailored technical assistance, services and resources to critical infrastructure organizations from all 16 critical infrastructure sectors based on the maturity of their respective cybersecurity programs. CISA seeks to collect this information from US critical infrastructure organizations on a strictly voluntary and fully electronic basis so that each organization can be best supported in meeting the CISA Cybersecurity Performance Goals. The CISA Cybersecurity Performance Goals are a set of 38 voluntary controls which aim to reduce the risk of cybersecurity threats to critical infrastructure. CISA offers a number of services and resources to aid critical infrastructure organizations in adopting the Cybersecurity Performance Goals and seeks to make discovery of the appropriate services and resources as easy as possible, especially for organizations that many have cybersecurity programs at low levels of capability. For example, an organization that is unsure of its ability to enumerate all its assets with Internet Protocol addresses can leverage CISA's highly scalable vulnerability scanning service to discover additional assets within its network range that may have been previously unknown. Organizations with more mature cybersecurity programs who wish to evaluate their network segmentation controls will be better positioned to take advantage of CISA's more resource-intensive architecture assessments. To measure adoption of the Cybersecurity Performance Goals and assist organizations in finding the best possible services and resources for their cybersecurity programs, CISA is seeking to establish a voluntary information collection that uses respondents' answers to tailor a package of services and resources most applicable for their level of program maturity. Without collecting this information, CSD VM will be unable to tailor an appropriate suite of

services, recommendations, and resources to assist that organization in protecting itself against cybersecurity threats, thereby creating burdens of inefficiency for service requesters and CSD VM alike. In addition, this information is critical to CSD VM's ability to measure the adoption of CISA's Cybersecurity Performance Goals by critical infrastructure organizations and assess the maturity of critical infrastructure organizations' cybersecurity programs. The information to be collected includes: whether an organization keeps a regularly updated inventory of all assets with an Internet Protocol address; the types of incident reporting and vulnerability disclosures required by an organizations' contracts with its vendors and suppliers; the minimum password strength required for all password-protected assets; and more.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;
2. Evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used;
3. Enhance the quality, utility, and clarity of the information to be collected; and
4. Minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, e.g., permitting electronic submissions of responses.

Analysis:

Agency: Cybersecurity and Infrastructure Security Agency (CISA), Department of

Homeland Security (DHS)

Title: CISA CyberCare

OMB Number:

Frequency: Upon each voluntary request for technical assistance, which CISA expects to occur on an annual basis.

Affected Public: Critical Infrastructure Owners & Operators seeking CISA services

Number of Respondents: Approximately 2,000 per year

Estimated Time Per Respondent: 20 Minutes

Total Burden Hours: 666.7 Hours

Robert J. Costello,
Chief Information Officer,
Department of Homeland Security,
Cybersecurity and Infrastructure Security Agency.

[FR Doc. 2023-12165 Filed: 6/6/2023 8:45 am; Publication Date: 6/7/2023]